GROUPEMENT DE GENDARMERIE DU VAUCLUSE
Cellule Prévention situationnelle

26 mars 2020

MESSAGE D'ATTENTION SÉCURITÉ ÉCONOMIQUE

Mise en garde escroquerie aux faux ordres de virement (FOVI)

Depuis l'apparition de ce nouveau type d'escroquerie en 2010, les faux ordres de virement (FOVI) appelés également « ***Fraudes au président*** » ont fait de nombreuses victimes parmi les entreprises françaises.

Dans le contexte de la crise sanitaire actuelle, il est constaté une recrudescence de faits commis au préjudice de sociétés françaises spécialisées dans le secteur de la santé pour ce qui concerne le commerce de produits pharmaceutiques notamment.

Principalement réalisée par téléphone ou par mail, l'escroquerie aux faux ordres de virement concerne les entreprises de toutes tailles et de tous les secteurs. Cela peut donc impacter tous les établissements en lien avec la santé.

C'est pourquoi, afin de permettre aux entreprises contribuant ou présentant un intérêt pour la santé publique de s'en prémunir, il apparaît nécessaire de sensibiliser les dirigeants de ces sociétés situées en ZGN à ce type de faits.

Définitions

« Fraude au président » : Cette escroquerie consiste à convaincre le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers pour obéir à un prétendu ordre du dirigeant, sous prétexte d'une dette à régler, de provision de contrat ou autre.

« Changement de RIB » : Cette fraude consiste à envoyer un mail à un salarié du service de comptabilité ou trésorerie de l'entreprise en se faisant passer pour un fournisseur, et lui demander de diriger ses versements vers un autre compte bancaire appartenant aux escrocs.

Souvent situés à l'étranger, les escrocs collectent en amont un maximum de renseignements sur l'entreprise. Cette connaissance de l'entreprise associée à un ton persuasif et convaincant est la clé de réussite de l'arnaque. L'opération est alors lancée sur les personnes capables d'opérer les virements (services comptables, trésorerie, secrétariat...).

La technique des fraudeurs est basée sur l'ingénierie sociale (ou « social engineering ») méthode qui a pour but d'extirper des informations à des personnes sans qu'elles ne s'en rendent compte. La clé étant la force de persuasion.

Quelques précautions à prendre

- **Rappeler à l'ensemble des collaborateurs** la nécessité d'avoir un usage prudent des réseaux sociaux privés et professionnels. Les alerter sur l'importance de ne pas y divulguer d'informations concernant le fonctionnement de l'entreprise.

- Sensibiliser **régulièrement l'ensemble des employés des services comptables, trésorerie, secrétariats, standards**, de ce type d'escroquerie. Prendre l'habitude d'en informer systématiquement les **remplaçants** sur ces postes.
- **Instaurer des procédures de vérifications** et de signatures multiples pour les paiements internationaux.
- Rompre la chaîne des mails pour les courriers se rapportant à des virements internationaux en **saisissant soi-même l'adresse habituelle du donneur d'ordre**.
- Maintenir à jour le système de sécurité informatique.
- Accentuer la vigilance sur les **périodes de congés scolaires**, les **jours fériés** et les **jours de paiement des loyers (facturation)**.

🗣 Reconnaitre les signes d'une attaque

- Une **demande de virement à l'international, non planifiée**, au caractère **urgent** et **confidentiel** : dans ce cas, contacter son interlocuteur habituel avec les coordonnées connues de la société.
- **Se méfier de tout changement de coordonnées téléphoniques ou mails**. Attention, la communication d'un nouveau numéro à l'indicatif français n'est pas une garantie.
- **Se méfier d'un contact direct d'un escroc se faisant passer pour un membre de la société ou un responsable qui va faire usage de flatterie ou de menace dans le but de manipuler son interlocuteur.**
- Pour asseoir sa crédibilité et usurper une fonction, **l'escroc apportera une abondance de détails sur l'entreprise et son environnement** : données personnelles concernant le chef d'entreprise, ses collaborateurs...

En cas de doute, prendre attache directement avec la personne au sein de la société, soit physiquement soit avec les coordonnées connues de l'entreprise.

🗣 Si vous êtes victime

- **Demander** immédiatement à la banque le **retour des fonds**.
- **Déposez plainte** rapidement en vous rendant dans le service le plus proche de votre domicile ou celui du siège de votre établissement ou encore sur le site institutionnel accessible depuis le lien suivant : *https://www.pre-plainte-en-ligne.gouv.fr/*
- Notez tout renseignement concernant l'appel et l'appelant.
- Conservez les courriels reçus et tout autre document reçu ou envoyé.

Un dépôt de plainte rapide permet d'optimiser les chances de récupérer les fonds escroqués.

NE PAS DÉPOSER PLAINTE
PERMET AUX AUTEURS DE POURSUIVRE LEURS ACTIVITÉS DÉLICTUELLES
EN TOUTE IMPUNITÉ

🗣 Pour aller plus loin

Retrouvez la gendarmerie sur Facebook a l'adresse :

- **Gendarmerie de Vaucluse**

Plus d'informations sur les référents sûreté :

- https://www.referentsurete.fr/